Comments to the U.S. Department of State

In response to Public Notice 8086, the State Department Sanctions Information and Guidance issued on November 8, 2012

COMMENTS OF ACCESS NOW, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, COLLIN ANDERSON, THE COMMITTEE TO PROTECT JOURNALISTS, AND THE NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE WITH REGARD TO THE GUIDANCE ON "SENSITIVE TECHNOLOGY"

January 12, 2013

EXECUTIVE SUMMARY

The undersigned coalition of civil society organizations welcomes the Department of State's Guidance on "Sensitive Technology". This guidance is an important effort to further clarify existing sanctions regulations and to make them more targeted. We appreciate the opportunity to comment and have outlined a set of recommendations to improve sanctions regulations that also have implications both for the export control regime and regulations administered by the Department of Treasury and the Department of Commerce.

We are aware that some of the elements in the Guidance are already covered by existing regulations, yet it is critical to further clarify the parameters of "sensitive technology." This clarification can not only improve sanctions regulation to prevent the transfer of network technologies that can facilitate human rights abuses, but also can ensure that technologies that promote free and secure expression are available to individuals living under sanctioned regimes. We continue to be concerned that some of the technologies that promote free expression may be inaccessible as a result of over-compliance by vendors under the existing sanctions. Clarifying the breadth of "sensitive technology" and creating more responsive government processes can help to address this problem and resolve legal uncertainty. We also consider the proposed refinements useful in order to apply special penalties for companies that are evading the existing sanctions to sell products that fall into the category "sensitive technology." Moreover, we want to highlight the potential transshipment of "sensitive technology" and recommend delineating technology transfers between third-party nationals and the sanction country based on explicit red flags and "know your customer" policies.

From a broader perspective, the concept of "sensitive technology" is useful but, in its current form, limited to sanctions countries. Many open questions remain regarding the export of "sensitive technology" to countries that are not on the sanctions list but with similarly questionable human rights records. We make some preliminary suggestions in this regard.

Specifically, we recommend that the Department of State:

- Revise the proposed terminology for the list of "sensitive technology" in order to more precisely define the function of significantly infringing equipment;
- Conceptualize dual use technologies as carrying a presumption of denial, wherein regulators or vendors limit the export of such goods to Iran and Syria unless it is clear that they will be utilized without contributing to repressive activities;
- Provide a set of red flags to identify and further investigate individual suspicious transactions in cases of the sale of physical goods or transactions conducted through negotiated sales;
- Provide more guidance as to what "rigorous due diligence" might involve and the context by which "know your customer" is to be understood with detailed suggestions outlined in our response below;
- Explicitly include after-sales knowledge with regard to due diligence;

- Emphasize that “know your customer” encompasses “know your reseller” and “know your regional partners,” including but not limited to direct inquiries into the reseller's or partner's business with entities of concern in Iran or Syria;
- Integrate discrete chapters on Internet Freedom within its annual Human Rights Reports as a source of information on states’ behavior.

Moreover, recognizing that the Department of State has limited role in licensing process itself, we recommend that the Department of State work with other relevant federal agencies to implement consistent reforms, including:

- Codify the U.S. government’s efforts to protect access to technology essential for ordinary network operation, personal computing or private communications in a broader General License within the Treasury’s export regulations, extending the previous authorizations for personal communications services to include commercial products and hardware;
- Ensure that any existing or future regulation pertaining to controlled technology allows for exemptions similar to those provided by TSU License Exception (15 C.F.R. 740.13), permitting allowances for open source or free and publicly-available software;
- Streamline and expedite the licensing process, with modifications that include implementing a 30-day time limit for license applications to be considered;
- Conduct recurring outreach to industry and civil society in order to ensure that federal agencies’ efforts match the fast pace of technological development, as well as changes in the methods used by infringing parties to bypass export controls.

I. INTRODUCTION

Beginning with the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA), the United States government has prohibited the export of goods or services that the government has designated as "sensitive technology"—those used to restrict or disrupt the free flow of information—to Iran. The U.S. government subsequently expanded these regulations to include Syria and to include stronger repercussions through legislative and administrative actions such as the Iran Threat Reduction and Syria Human Rights Act of 2012 (TRA), Executive Order 13606 (the GHRAVITY E.O.) and Executive Order 13628. In consideration of the importance of these efforts, we offer the following comments on the Proposed Guidance concerning the Provision of "Sensitive Technology" to Iran and Syria. In order to support efforts to protect free expression and access to information, we seek to clarify the obligations of private vendors; highlight differences between more clear cut infringing technology and potential cases of "dual use"; offer suggestions for balancing policy objectives; and outline potential due diligence processes to increase knowledge about the end-users of the technology.

Supporting Access While Regulating Sensitive Technologies

We remain concerned with the balance between enabling the development of information infrastructure and the sustained sale of surveillance equipment to entities that have substantial ties to governmental institutions.

American and European sanctions currently create strong barriers to prevent the further sale of lawful interception capabilities by their citizens to any party in Iran or Syria, in accordance with the proposed guidance and text of the TRA. Moreover, third party nationals may be subject to licensure requirements if they use U.S. banks or if *de minimis* rules apply. In addition, these transactions may be designated as human rights violations under Executive Orders 13606 and 13628. Therefore, the Departments of State and Treasury maintain the responsibility to define a set of practices that are applicable internationally, while respecting the gravity of both mandates.

The Department of State's Proposed Guidance takes significant steps to identify both the technologies and applications of technologies that warrant heightened scrutiny from vendors, while acknowledging the need to protect access to technology essential for ordinary network operation, personal computing, or private communications. The Department of Treasury should follow these constructive developments by codifying a broader General License within export regulations that extends the previous authorizations for personal communications services to include commercial products and hardware. Currently, ambiguities in licensing guidelines have created a chilling effect. When private entities respond to sanctions through over-compliance, that behavior closes vital channels for free expression and access to information. Through explicit legal authorizations for these fundamental tools, federal agencies can increase the sanctions' effectiveness by making them more targeted. This will ensure that legitimate enforcement and regulatory activities do not send unintended signals to private companies and potentially undermine their overarching foreign policy goals.

All relevant agencies should take steps to streamline and expedite the licensure process. These modifications should include implementing a set 30-day period for license applications to be considered. Without this and other improvements, the uncertainty and burdensome length of the licensing process will remain a serious disincentive for companies to act in good faith or make essential personal communications services and tools available to individuals living under authoritarian regimes.

There is little evidence to suggest that the governments of Iran and Syria would permit information networks that did not include surveillance and censorship capacities. As demonstrated by those governments' throttling of connectivity and regulatory restrictions on the availability of broadband connections, it is clear that they would prefer to deny their populations access to the Internet and its social development capacity, rather than potentially lose control. By defining technologies in an overbroad manner, or defining telecommunications companies under sanctions, without consideration of outstanding circumstances, controls may inadvertently exacerbate the restrictiveness of repressive governments. In other words, this could result in ordinary citizens being denied access to critical telecommunications or other technology. In parallel, special attention should be paid to ensure that definitions control the end purpose of infringing activities to ensure that vendors of sensitive technologies cannot bypass export regulations by slightly modifying means or approach. Therefore, there is a need to delineate technology transfers between third-party nationals and Iran based on explicit red flags and "know your customer policies," while carving out "bright lines" for "positive"[1] list of technologies which can be used to violate human rights in authoritarian environments.

Further clarity on the availability of technology through the delineation of bright lines on categories of technology, red flags on potential transactions, and guidance for dual use scenarios can be detailed by policy makers without introducing rigidity that stifles enforcement or overburdens vendors. However, considering the broader issues of liability, academic freedom and the difficulty of restricting availability, any regulation pertaining to controlled technology should allow for exemptions similar to those provided by TSU License Exception[2] permitting allowances for open source or publicly-available software. Finally, it is important to bear in mind the need for broader restrictions on the export of sensitive technologies globally. The continued leakage of this technology through third parties, the dangers of their further proliferation or international acceptance, and the direct threat posed by their presence in any state with a history of violating human rights codified within international law make such consideration a necessity.

[1] The term "positive" is used in its denotation similar to "explicit" as commonly used in the context of export regulations.

[2] "License Exceptions: Technology and Software - Unrestricted," 15 C.F.R. 740.13

II. TECHNOLOGIES

Technologies for Significant Controls ("Bright Lines")

The Proposed Guidance highlights a number of technologies that have limited legitimate application in states with a questionable human rights record. While the trend of regulating based on the circumstances of the export is necessary to handle problems of "dual-use" technologies, for particularly malicious devices high barriers still need to be erected through explicit controls to limit their availability. Such control should be based upon objective criteria or parameters of the specifications of the technology, rather than broad, open-ended or subjective criteria.

We begin to define "sensitive technologies" as those that may be used for any of the following infringing purposes:

- Interception of private communications;
- Compromise, theft, destruction, or manipulation of privately held data;
- Censorship of online communications and platforms;
- Interference and disruption of standard network operations;
- Acquiring access to computer, telephone, and other telecommunications equipment without the consent or knowledge of the owner;
- Surveillance, lawful interception capabilities;
- Non-consensual tracking of physical location and behaviors.

We agree with the spirit of the technologies enumerated in the guidance to be considered as "bright lines." We only find a need to address minor definitional issues in order to more precisely define the function of significantly infringing equipment, as well as shifting some technologies into a list of dual use goods.

> **Proposal from State: "**Mobile device forensics data extraction and analysis technology: Allows persons to extract and analyze data from a mobile phone device, even if password protected."
>
> **Recommended Language:** "Mobile Device Data Extraction Technology: Hardware and software that allows for the non-consensual bypassing of security measures and extraction of data stored on a mobile device."
>
> **Proposal from State:** "Key logging technology / spyware: Allows persons to record keystrokes, mouse clicks, data processes, or activity on a touchscreen without consent of the device user.*"*

Recommended Language: "Tactical Malware, Keylogging Technology and Spyware: Software and hardware designed for the surreptitious, non-consensual control and collection of device usage, manipulating and recording user input, such as device data and processes, account credentials, device sensors, camera operations, and telephony activities."

Proposal from State: "Nonconsensual tracking/monitoring technology: Allows persons to cause a mobile or networked device to reveal its geographic location, operating status or application data, without consent of the device owner or content provider."

Recommended Language: "Non-consensual Tracking or Monitoring Technology: Equipment designed for the purposes of causing a mobile or networked device to reveal its geographic location, operating status, equipment or application data, or allow for the surreptitious interception of data and voice traffic, without consent of the device owner or content provider, such as through creating a localized mobile network."

Proposal from State: "Network disruption technology: Designed to enable disruption, inhibition or degradation of networks or sub-parts."

Recommended Language: "Network disruption technology: Technology specifically designed to enable disruption, inhibition or degradation of communications networks or the transmission of information between devices."

Proposal from State: "Infection vectors technology: Allows persons to install or execute malware or perform other attacks."

Recommended Language: "Non-Consensual Access and Privilege Escalation Mechanisms: Technology, rootkits or backdoors designed for the purposes obtaining non-consensual third-party access to devices and services, for objectives such as the installation of malware or other attacks."

Note: *We remain unclear as to the distinction between the Proposed Guidance's categories of "non-consensual remote forensic technology" and "rootkit" from a holistic definition of malware and unauthorized access mechanisms. Further clarity may be required to ensure application on the technologies envision by the Department of State.*

Additional Comments on Dual Use Technologies

Considering the breadth of both beneficial and malicious use cases, there are substantial areas in which the Department of State should avoid deploying "bright line" tests in order to

accommodate differences in circumstances of deployment or in the potential uses of technologies. For example, after Blue Coat network appliances were found to be used for censorship in Syria, the company noted that their devices were not designed for surveillance purposes. Furthermore, significant attention has been given to accounts of the use of Deep Packet Inspection (DPI) in Iran for the purposes of interfering with anti-filtering tools and monitoring political activists. As with any network caching device, such equipment is capable of both legitimate, modern network purposes of blocking malware and reducing load, as well as infringing activities such as logging traffic and filtering political content. DPI has an established utility in ensuring the information security of businesses and protecting users. But this application of the technology can be differentiated from a potentially infringing situation, based on the user, use case and operational details of the attempted export.

Dual use technologies should therefore carry a presumption of denial, wherein regulators or vendors limit the export of such goods to Iran and Syria unless it is clear that they will be utilized without contributing to repressive activities. Based on historical cases such as Blue Coat, it may be useful within the Final Guidance to provide an additional illustrative, but not exclusive, list of technology for which vendors bear a substantial degree of responsibility to ensure that they are not used by authoritarian governments for the purpose of perpetrating human rights abuses. Such a list might include:

- Pattern Recognition, Semantic Processing and Pattern Profiling Equipment: Technology used for the purposes of surreptitiously identifying individuals and relationships based on audio, visual, locational or other data;

- Deep Packet Inspection-based interception and monitoring equipment;

- Network caching appliances;

- Cryptanalysis Equipment: Equipment specifically designed to break and perform cryptanalysis on privacy-preserving encryption, such as AES, RSA, WEP or WPA;

- GPS Tracking Devices: GPS for non-consensual tracking of individuals;

- Keyword Blocking Technology: Equipment that allows intermediaries to block the transmission of messages or availability of content based on certain words or rules;

- Censorship-Enhancement Technology: Generally designed to allow persons to enforce content blocking or to fingerprint and/or defeat anti-censorship technologies;

- Man-in-the-Middle Attack Vectors: Equipment intended to facilitate surveillance and censorship through performing man-in-the-middle attacks on large networks, including DNS cache poisoning, interception of SSL-based communications, or interception of network traffic without the knowledge, consent, or control of the user.

It is important to bear in mind that while the proposed guidance clearly states that the definition of "sensitive technology" does not generally include technology essential for ordinary network operation, this line is often blurred by not only notions of "dual use" but also by the less technical issues of contractual arrangements. Companies that wish to continue to provide

telecommunications services to Iran are almost certainly required to comply with "lawful interception" demands, as the government and vendor assert as a legitimate right under the Constitution of the International Telecommunication Union.[3] However, we believe that the Final Guidance should continue to strongly restrict "'lawful interception" and "surreptitious listening" devices, particularly those provided by Western vendors and when made available as discrete components. The issue is further complicated by the fact that telecommunications infrastructure is frequently sold within "product bundles" that include surveillance capability as a component, and buyers require such capacities within bids for contracts and spectrum licensing.

III. KNOW YOUR CUSTOMER

> *"When making an assessment of whether or not a company, entity, or individual is exporting, transferring, facilitating the transfer of, or providing services that may be considered sensitive technology with regard to Iran or Syria, the State Department will review all available information, including through direct communication with the entity or individual if possible. It will consider, among other factors, whether a company knew, or should have known, that a particular end-user of its technology was likely to misuse such technology, or that a particular technology has a history of being misused in Iran or Syria to further human rights abuses. As such, individuals or entities engaged in transactions with Iran or Syria involving telecommunications goods, services or technology should conduct rigorous due diligence to "know their customer" and assess the potential risk that a particular technology is likely to be used to facilitate human rights abuses, restrict the free flow of information, or disrupt, monitor, or otherwise restrict speech of the people of Iran and Syria."*
>
> (Source: http://www.state.gov/e/eb/tfs/spi/iran/fs/200316.htm)

We strongly agree that the scope of the term "sensitive technology" is as dependent on the end-user and predicted end use as it is on the type and capabilities of the technology under consideration. Given this distinction, we feel that more guidance could be given as to what "rigorous due diligence" might involve, and the context by which "know your customer" is to be understood. In particular, our experiences with the current deployment and detection of the technologies listed,[4] as well as the self-assessments conducted by technology companies, offers some procedures that may instruct that guidance.

---

[3] "Chinese Tech Giant Aids Iran", Wall Street Journal, October 27, 2011
http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html
[3] "Technical Aspects of Lawful Interception" , International Telecommunication Union, May 2008, p.1 foonote #3
http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000060002PDFE.pdf
[4] For references, see:

- [4] https://www.eff.org/deeplinks/2012/08/syrian-malware-post
- [4] https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software-2/
- [4] http://cpj.org/security/2012/02/caveat-utilitor-satellite-phones-can-always-be-tra.php
- [4] http://b.averysmallbird.com/entries/bluecoat-and-syria-indicators-and-culpability

"Know your customer" has two potential meanings in this context: 1) the requirements adopted by the international financial sector to require identification of potential clients[5] and monitoring of transactions to detect suspicious behavior, 2) or "know your customer" in the sense of the export administration regulations,[6] a process built around detecting and responding to a series of red flags developed by the Department of Commerce which could indicate a potentially suspicious transaction. Given that many of the sensitive technologies described can often involve both a one-off transaction (the sale of shrinkwrapped or downloadable software, as well as the transfer of hardware) and ongoing servicing thereafter, we recommend a combination of both approaches.

The following real world example is illustrative of the problem: According to an enforcement announcement by the Department of Commerce's Bureau of Industry and Security on December 15, 2011, Waseem Jawad, using the company name Infotec, ordered multiple Blue Coat proxy devices from an authorized distributor in the United Arab Emirates, and identified the order as destined for Iraq's Ministry of Communication.[7] These devices were then transferred to the Syrian Telecommunications Establishment to be used as core components of the regime's surveillance and censorship apparatus. Upon the discovery of these devices, Steve Schick, a Blue Coat spokesman, stated that "we see no firm evidence that would determine there is Blue Coat equipment in Syria; in fact, it appears that these logs came from an appliance in a country where there are no trade restrictions."[8] These statements were made in spite of evidence that the devices made calls to update its censorship database.

Entities should take steps to investigate, identify and exclude end-users who could use such technology to engage in infringing activities, but allow its transfer to those who are using the technologies to protect networks and facilitate expression. In evaluating whether a technology may be used for repressive purposes, companies, organizations or individuals should assess the likely end-use of a product with reasonable certainty. Such standard of reasonable certainty should, at a minimum, include assessment of the following elements:

- Design of the technology;
- Relationship with the contracting entity, including length of relationship and demonstrated reliability, with respect to export controls and sanctions compliance;
- Final country destination, recipient, and end use of the technology, such as location in a network or nature of the buyer, supported by clear and detailed documentation;

[5] 31 USC § 5318(h),(i),(l)

[6] "Know Your Customer Guidance", Bureau of Industry and Security, Department of Commerce, 16 Apr 2009, http://www.bis.doc.gov/complianceandenforcement/knowyourcustomerguidance.htm

[7] "BIS Address Two Parties to Entity List for Sending Internet Filtering Equipment to Syria", Bureau of Industry and Security, Department of Commerce, 15 December 2011, http://www.bis.doc.gov/news/2011/bis_press12152011.htm

[8] "Blue Coat Denies Its Devices Helping Syrian Gov't", Slashdot, 11 Oct 2011, http://yro.slashdot.org/story/11/10/11/1629238/blue-coat-denies-its-devices-helping-syrian-govt

- Extent of ongoing servicing of the technology, including potential for post-export checks on compliance.

The Commerce Department has developed lists of such red flags. These lists are not all-inclusive, but are intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate the EAR. Toward this end, BIS has provided a general set of recommendations, which are often clarified by further recommendations that are industry-specific.[9] In cases of the sale of physical goods or transactions conducted through negotiated sales, the Departments of State and Commerce should provide a set of red flags to help identify and further investigate individual suspicious transactions. Such due diligence should explicitly include after-sales knowledge. Both hardware and software, as part of its normal maintenance, failure diagnostic reporting, or update cycles, may communicate with its original manufacturer. Documentation, software and firmware updates may also be proactively downloaded by customers. These communications can indicate the location or usage patterns of such technology.

There is a risk that individuals or entities may "self-blind" by ignoring the location of such requests or the uses reflected by such requests, or disabling auto-update features at the request of Iranian or Syrian customers. To prevent this, it may be useful to indicate that such reports can be used to seek inclusion under the special rule to allow for the termination of sanctionable activity.[10]

Pertinent red flags may include:

- Originating IP Address for Software Updates;
- Traffic to indicate strong user bases originating from Iranian or Syrian locales;
- Registration information;
- Stated end use;
- Technical discussions or questions from potential customers;
- Requests for customization.

The United Nations Guiding Principles on Business and Human Rights' operational principles regarding corporate responsibility to respect human rights and remedy abuses also provides a general institutional framework.[11]

---

[9] See example, "Best Practices for Preventing Unlawful Diversion of U.S. Dual-Use Items subject to the Export Administration Regulations, Particularly through Transshipment Trade"

[10] 22 USC § 8515a(b)(3), 'Iran Threat Reduction and Syria Human Rights Act of 2012', Sec. 703 (b)(3).

However, as with the cryptography export restrictions, the general publication of any mass market software on the Internet for free and anonymous download should not serve as a basis for sanction, even though routine logging occurs. See 15 C.F.R. sec. 740.13 et. Sequ.

[11] "UN Guiding Principles on Business and Human Rights" http://www.business-humanrights.org/Documents/UNGuidingPrinciples (II.B.16-24)

We would like to specifically highlight the potential for the transshipment of prohibited transactions conducted by authorized third parties, such as resellers or regional partner organizations. The TRA reinforces that vendors have critical responsibilities within its prohibitions on "facilitat(ing) the transfer" and the post-export support of sensitive technologies. Therefore, it should be emphasized within the Final Guidance that "know your customer" encompasses "know your reseller" and "know your regional partners," including but not limited to directed inquiries into the reseller's or partner's business with entities of concern in Iran or Syria. Regional entities and third-parties may be unaware of the liabilities that the original vendor may incur and legal responsibilities that they retain.

Potential language for this clarification could come from the Global Network Initiative's implementation guidelines on responsible company decision making.[12] The Global Network Initiative, whose members include Microsoft, Yahoo, Google, Websense, and Evoca, has worked with its corporate members to develop processes and procedures to identify circumstances where freedom of expression and privacy may be either jeopardized or advanced through the offering of technology and services. This work includes human rights impact assessments in regions "where the risk to free expression and privacy is at its greatest." For instance, GNI practice has shown the value of these assessments during the development of new products and services in order to design safeguards against their misuse in Iran, Syria, and other regions. More detailed suggestions on a "Know Your Customer" regime appropriate for censorship and surveillance technologies have also been documented by the Electronic Frontier Foundation.[13]

Furthermore, recurring outreach to industry and civil society should be conducted in order to ensure that federal agencies' efforts match not only the fast pace of the technological development, but also changes in the ways infringing parties may attempt to bypass controls. This cross-sector collaboration should begin through the establishment of a normative set of red flags used to evaluate potential technology transfers and the obligations of vendors post-shipment. The Department of State may also frame this initiative in the context of a discrete chapter on Internet Freedom within its annual Human Rights Reports. More broadly, these engagements should coordinate the sharing of expertise and experiences, mitigating potential information gaps in enforcement, and improving feedback for civil society initiatives, such as "know your customer" frameworks.

IV. CONCLUSION

As organizations concerned with protecting the free flow and unfettered access to information in repressive environments, we recognize and appreciate that, through the Proposed Guidance, the Department of State has sought to begin to address long-standing concerns about the impact on technology exports to environments where they will facilitate human rights abuses. We are optimistic that through broad, engaged coordination with civil society and the business sector, federal agencies can play a constructive role in establishing and reinforcing global norms

[12] http://globalnetworkinitiative.org/implementationguidelines/index.php

[13] See https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

on the export of potentially "sensitive technologies." We therefore urge the Department of State to consider carefully all comments received regarding the Proposed Guidance in order to develop an approach that will provide clear guidance for international entities that minimizes the availability of sensitive technology, while protecting the development of the infrastructure on which the information technology revolution is predicated.